Definitions

Please refer to the “Software Independent Verification and Validation (IV&V) Independent Assessment (IA) Criteria” document under “Help” on the web site menu bar for additional clarification.

Factors contributing to the consequences of software

Potential for loss of life.

Is the software the primary means of controlling or monitoring systems that have the potential to cause the death of an operator, crewmember, support personnel, or bystander? The presence of manual overrides and failsafe devices are not to be considered. This is considered a binary rating: responses must be either yes or no. Examples of software with the potential for loss of life include:

- Flight and launch control software for manned missions
- Software controlling life support functions
- Software controlling hazardous materials with the potential for exposure to humans in a lethal dose
- Software controlling mechanical equipment (including vehicles) which could cause death through impact, crushing, or cutting
- Any software which provides information to operators where an inaccuracy or misinterpretation of the data could result in death through an incorrect decision (e.g., mission control room displays)

Potential for serious injury.

Serious injury is here defined as loss of digit, limb, or sight in one or both eyes, sudden loss of hearing, or exposure to substance or radiation that could result in long term illness. This rating is also binary. This rating considers only those cases where the software is the primary mechanism for controlling or monitoring the system. The presence of manual overrides and failsafe devices are not to be considered. Examples of software with potential for serious injury include software controlling milling or cutting equipment, class IV lasers, or X-ray equipment.

Potential for catastrophic mission failure.

Can a problem in the software result in a catastrophic failure of the mission? This is a binary rating. Software controlling navigation, communications, or other critical systems whose failure would result in loss of vehicle or total inability to meet mission objectives would fall into this category.

Potential for partial mission failure.

Can a problem in the software result in a failure to meet some of the overall mission objectives? This is a binary rating. Examples of this category include software controlling one of several data collection systems or software supporting a given experiment, which is not the primary purpose of the mission.

Potential for loss of equipment.

This is a measure of the cost (in dollars) of physical resources that are placed at risk due to a software failure. Potential collateral damage is to be included. This is exclusive of mission failure. Examples include:

- Loss of a $5 million unmanned drone due to flight control software failure. (Assuming the drone is replaceable, this wouldn't be a mission failure)
- Damage to a wind tunnel drive shaft due to a sudden change in rotation speed.

Potential for waste of software resource investment.

This is a measure or projection of the effort (in work-years, civil service, contractor, etc.) invested in the software. This shows the level of effort that could potentially be wasted if the software doesn't meet requirements.

Potential for adverse visibility.

This is a measure of the potential for negative political and public image impacts stemming from a failure of the system as a result of software failure. The unit of measure is the geographical or political level at which the failure will be common knowledge-specifically: local (Center), Agency, national, international. The potential for adverse visibility is evaluated based on the history of similar efforts.

Potential effect on routine operations.

This is a measure of the potential to interrupt business. There are two major components of this rating factor: scope and impact. Scope refers to who is affected. The choices are Center and Agency. The choices for impact are inconvenience and work stoppage. Examples:

- A faulty firewall which failed to protect against a virus resulting in a 4-hour loss of e-mail capabilities at Goddard would be a "Center inconvenience".

- Assuming that the old financial management software was no longer maintainable, the failure of the replacement system to pass acceptance testing and the resulting 2-year delay would be a potential "Agency work stoppage." This doesn't imply that workarounds couldn't be implemented, but only that it has the potential to stop work Agencywide.